UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/518,416	03/03/2000	Robert Huijie Deng	U 012638-5	6305

140 7590 02/27/2004

LADAS & PARRY
26 WEST 61ST STREET
NEW YORK, NY 10023

EXAMINER	
HENEGHAN, MATTHEW E	
ART UNIT	**PAPER NUMBER**
2134	10

DATE MAILED: 02/27/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/518,416	DENG ET AL.	
	Examiner	Art Unit	
	Matthew Heneghan	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *20 January 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *75-106* is/are pending in the application.

4a) Of the above claim(s) *91-106* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *75-90* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *03 March 2000* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *3.4.16*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 75-90 have been examined. Claims 91-106 have withdrawn from consideration in response to an election requirement issued by the Office (see Paper No. 17) without traverse.

Priority

2. The instant application claims priority to Singapore Patent Application No. 9906598-9, filed 24 December 1999.

Information Disclosure Statement

3. The following Information Disclosure Statements in the instant application have been fully considered:

Paper No. 3, filed 15 May 2000.

Paper No. 4, filed 16 June 2000.

Paper No. 16, filed 28 February 2003.

Drawings

The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because they include the following reference sign(s) not mentioned in the description:

figure 2, item 200; figure 3, item 300; figure 4, item 400. A proposed drawing correction, corrected drawings, or amendment to the specification to add the reference sign(s) in the description, are required in reply to the Office action to avoid abandonment of the application. The objection to the drawings will not be held in abeyance.

Specification

4. The abstract of the disclosure is objected to because the phrase "FIG. 6" in line 15 does not belong in the abstract. Correction is required. See MPEP § 608.01(b).

Claim Objections

5. Claims 77, 81, 85, and 89 are objected to because of the following informalities: They are not single sentences. Appropriate correction is required.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

6. Claim 76, 80, and 84 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

The phrase "such as" renders the claim indefinite because it is unclear whether the limitations following the phrase are part of the claimed invention. See MPEP § 2173.05(d). For purposes of the prior art search, the limitations following "such as" are being ignored.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claim 75, 77-79, 81-83, 85-87, 89, and 90 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 5,440,635 to Bellovin et al. in view of Dwork et al., "Concurrent Zero-Knowledge," 1998.

Regarding claims 75, 78, 79, 82, 83, 86, 87, and 90, Bellovin discloses a remote public key authentication protocol using the Diffie-Hellman key exchange wherein Alice and Bob exchange challenge and response signals (ciphertexts) using their respective keys, along with their respective keys, using a symmetric algorithm. Each party then computes the session key based on the products of the respective random numbers to complete the transaction, and exchange authentication and validation signals and verify them (see entire Detailed Description).

Bellovin does not incorporate the usage of an elapsed time test in the authentication procedure.

Dwork discloses the usage of time constraints in key exchange procedures, where the length of time for a transaction must be above a minimum but below a maximum range, and bases the range on message length (see section 4, Protocol III, for example). Dwork suggests that this enables the obtaining of zero-knowledge in concurrent executions (see abstract).

Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to modify the protocol disclosed by Bellovin to include time constraints on transmissions by each party, as disclosed by Dwork, in order to obtain zero-knowledge in concurrent executions.

Regarding claims 77, 81, 85, and 89, official notice is given that the technique of recognizing another party by familiar biometric characteristics (such as a friend's voice) is well-known in the art to be a quick and easy way to verify an identity.

Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to further modify the protocol of Bellovin and Dwork by also recognizing another party's familiar characteristics, as is well-known in the art, as a quick and easy way to verify an identity.

8. Claims 76, 80, 84, and 88 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 5,737,420 to Tomko et al. in view of U.S. Patent No. 5,440,635 to Bellovin et al. in view of Dwork et al., "Concurrent Zero-Knowledge," 1998.

Tomko discloses a method for biometric key exchange wherein the key exchange may be based on a Diffie-Hellman key derivation, but does not disclose a specific method for the key exchange (see column 2, lines 42-64).

Bellovin and Dwork disclose a Diffie-Hellman key exchange, as described above. Bellovin further suggests that the method is useful because it protects the information from being revealed to an eavesdropper.

Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to implement the Diffie-Hellman key exchange in the invention of Tomko using the technique disclosed by Bellovin and Dwork, in order to protect the information from being revealed to an eavesdropper.

Conclusion

9. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

U.S. Patent No. 4,710,613 to Shigenaga discloses an authentication system wherein authentication information is validated by comparing against the predicted processing time for a challenge.

U.S. Patent No. 5,491,750 to Bellare et al. discloses methods for key exchanges in establishing encrypted connections.

U.S. Patent No. 5,720,034 to Case discloses a method for generating identical keys for both users.

U.S. Patent No. 5,910,989 to Naccache discloses key signature authentication based upon response time.

U.S. Patent No. 6,571,344 to Sitnik discloses a method for authentication based upon response time.

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew E. Heneghan, whose telephone number is (703) 305-7727. The examiner can normally be reached on Monday-Thursday from 8:00 AM - 4:00 PM Eastern Time. The examiner can also be reached on alternate Fridays.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse, can be reached on (703) 308-4789.

Any response to this action should be mailed to:
Commissioner of Patents and Trademarks
P.O. Box 1450
Alexandria, VA 22313-1450
Or faxed to:
(703) 872-9306
Hand-delivered responses should be brought to Crystal Park 2, 2121 Crystal Drive, Arlington, VA 22202, Fourth Floor (Receptionist).

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

MEH

February 10, 2004